AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

DETACHED GARAGE/LIVING SPACE LOCATED BEHIND THE MAIN RESIDENCE AT 1212 DERIDDER STREET, FORT WORTH, TX 76106

Case No. 4:19-MJ- 808

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Further described in Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

Further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 471	Forging and Counterfeiting Currency
18 U.S.C. § 473	Dealing in Counterfeit Currency

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

S. Taylor Turnbow, Special Agent, USSS
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/10/19

Judge's signature

City and state: Fort Worth, Texas

Jeffrey L. Cureton, U.S. Magistrate Judge
Printed name and title

IN THE MATTER OF THE SEARCH OF A DETACHED GARAGE/LIVING SPACE LOCATED BEHIND THE MAIN RESIDENCE AT 1212 DERIDDER STREET, FORT WORTH, TX 76106	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, S. Taylor Turnbow being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the above referenced premises which is more thoroughly described in Attachment A.

2. I have been employed as a Special Agent with the United States Secret Service (USSS) since July 2000. I am currently assigned to the Criminal Investigations Squad in the USSS Dallas Field Office. My duties include investigating violations of United States currency laws, including counterfeiting, money laundering, financial fraud, and forgery of U.S. securities. The information contained in this affidavit is based upon observations and an investigation conducted by me, other USSS Special Agents, and state and local law enforcement Officers.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE PREMISES TO BE SEARCHED

4. The property to be searched is a detached garage which has been converted into a living space, situated in the rear of the property located at 1212 Deridder Street in Fort Worth, TX (Hereinafter PREMISES) in the Northern District of Texas, and further described in Attachment A incorporated with this affidavit.

5. The applied-for warrant would authorize the search of the PREMISES, including any computers, computer media, and wireless telephone devices located therein, for the purpose of identifying evidence which constitutes proof of the commission of a criminal offense, contraband, the fruits of crime, and property, as more fully specified in Attachment B, designed or intended for use or which is or has been used as the means of committing a criminal offense, that is, making, forging and counterfeiting currency of the United States, and transferring false, forged, and counterfeited obligations or other securities of the United States in violation of Title 18, United States Code, Sections 471 and 473.

PROBABLE CAUSE

6. This case originated 8/27/19, upon receipt of Richland Hills PD Incident Report 19R12188 regarding the arrest of individuals with US counterfeit currency. A review of this report revealed the following:

7. On 8/18/19, a traffic stop was conducted by Richland Hills PD Patrol Officers at which time, Scott Sosa, the driver of the vehicle, was arrested for outstanding warrants. The passenger in the car was also arrested as the Officers located methamphetamines, drug paraphernalia and US currency in the vehicle. Both individuals were transported to the Richland Hills jail without incident. During the routine inventory of evidence and personal property,

Officers discovered that part of the money found was counterfeit Federal Reserve Notes (FRNs). The description of this counterfeit currency revealed that it consisted of two $100 FRNs bearing serial number KB34170997F; two $50 FRNs bearing serial number MB57615824C; two $20 FRNs bearing serial number MG83183418B; one $20 FRN bearing serial number ML25086362K and three $10 FRNs bearing serial number ML52769298A.

8. Continuing on 8/27/19, a query of the US Secret Service Counterfeit Tracking Database revealed multiple prior passes of each of these serial numbers in the DFW area dating back approximately one year.

9. On 8/28/19, SSA Burch and I interviewed Scott Sosa at the Tarrant County Detention Center. Prior to questioning, Sosa was advised of his Miranda rights, which he waived by signing SSF 1737. Sosa provided the following information related to this investigation:

10. Approximately a week prior, he and a friend were stopped by the Richland Hills PD for an inoperable tail light. He was arrested due to outstanding warrants and a probation violation. He said that the officers also found methamphetamines and counterfeit currency in a backpack inside the vehicle.

11. With respect to the counterfeit currency, Sosa claimed that it was received from an associate, Octavius Fernandez, AKA Junior, in exchange for a laptop computer. Sosa said that Fernandez lives on Deridder Street in Fort Worth, near the intersection with Decatur. He claimed Fernandez lives in a detached, converted garage behind the main house, where his parents reside. He said he has witnessed Fernandez manufacturing counterfeit currency at this location and that he had been doing it for about a year or so. He explained that Fernandez has multiple computers and printers in the room where he sleeps and that he manipulates the images on a computer and transfers them to a thumb drive which he connects to a printer to print the

counterfeit currency. He described Fernandez as a Hispanic male in his early 30's, approximately 5'9" and 200 lbs.

12. Continuing on 8/28/19, an NLETS query for Octavius Fernandez was negative. I was, however, able to locate Octavio Fernandez at 1212 Deridder Street in Fort Worth. Further investigation revealed that this address is a single family residence with a shed or garage in the back yard and that the owner and resident of the main house is Octavio Fernandez Sr. This information is consistent with the description of the property provided by Sosa. Texas Drivers License information for Octavio Fernandez Jr. revealed that he is 37 years old and fits the physical description provided by Sosa.

13. On 9/9/19, a Confidential Informant (CI20-02282) reported that contact was made with Fernandez and that he had agreed to provide additional counterfeit currency in exchange for genuine currency. He also agreed to meet with CI20-02282 at McDonald's restaurant, 3901 Airport Fwy in Fort Worth between 10:00 and 11:00 am on 9/13/19.

14. On 9/13/19, surveillance was initiated at 1212 Deridder Street in Fort Worth, the residence of suspect Fernandez. CI20-02282 was briefed at the Richland Hills Police Department and transported by a second Agent and me to the meeting location at approximately 9:30 am. Prior to departure from the Police Department, CI20-02282 was searched to ensure the absence of any weapons, money or contraband. CI20-02282 was provided $50 for the transaction. Other Agents and I positioned ourselves inside the restaurant to observe the meeting. Additional Agents were located in the parking lot. At approximately 11:15 am, the operation was terminated as suspect Fernandez failed to show up and he ceased communication with CI20-02282. CI20-02282 returned the buy money and was instructed to report any subsequent communication with Fernandez.

15. On 9/30/19, CI20-02282 advised that Fernandez had been in contact via text message offering to sell counterfeit currency. CI20-02282 set up a meeting with Fernandez for the afternoon of 10/1/19, and agreed to pay him $100 for $300 in counterfeit.

16. On 10/1/19, CI20-02282 met with myself and another Agent at a staging location in Fort Worth, TX prior to the scheduled meeting with Fernandez. CI20-02282 was searched to ensure the absence of any weapons, money or contraband. A disconnected non-working surveillance camera was discovered in CI20-02282's hand bag, which CI20-02282 advised was going to be given to Fernandez as part of the deal, explaining that Fernandez had repeatedly expressed interest in the camera. A Physical Security Specialist placed an audio transmitter in CI20-02282's hand bag along with an audio recorder. CI20-02282 was provided with $100 in genuine US currency and instructed to purchase as much counterfeit currency as possible from Fernandez.

17. CI20-02282 was driven to Fernandez's residence, 1212 Deridder Street in Fort Worth, TX. Upon arrival at approximately 1500 hours, CI20-02282 proceeded to the detached garage behind the residence, (PREMISES) where Fernandez lives. After repeated knocking, Fernandez opened the door and invited CI20-02282 inside. Conversation ensued regarding the counterfeit currency and the camera resulting in CI20-02282 receiving $650 in counterfeit currency in exchange for $100 in genuine currency and the aforementioned non-working camera. This meeting lasted approximately 10 minutes, at which time, CI20-02282 exited the garage and walked back to the transport vehicle. CI20-02282 was then transported back to the staging area where I took possession of the counterfeit currency (nine CFT $50 FRNs bearing serial number MB57615824C; seven CFT $20 FRNs bearing serial number MG83183418B; two CFT $20 FRNs bearing serial number ML25086362K and two CFT $10 FRNs bearing serial number

ML52769298A), along with a sheet of folded paper containing a white gelatinous substance that Fernandez claimed was Benadryl cream. CI20-02282 advised that Fernandez said to apply the cream to the counterfeit bills in order to prevent proper function of a counterfeit detection pen. The transmitter and recording devices were removed from CI20-02282. CI20-02282 was instructed to report any subsequent contact with Fernandez and subsequently departed the location.

18. On 10/2/19, a query of the Secret Service Counterfeit Tracking Database revealed prior history of all four of these serial numbers in the DFW area dating back approximately a year. It was also noted that these serial numbers match the numbers on the counterfeit previously recovered from Sosa pursuant to the aforementioned arrest by the Richland Hills PD.

19. In my training and experience, I have come to know that individuals engaged in manufacturing of counterfeit US currency often use computers and other electronic devices to facilitate their criminal activity. These electronic devices, including but not limited to computers, laptops, tablets, hard drives, flash drives, storage disks, printers, scanners, cameras, etc., are both instrumentalities of the crime and are known to contain evidence of the crime. In this case, there is probable cause to believe that electronic equipment found at the PREMISES has been used to commit or facilitate this crime and will contain evidence of the crime based on statements by Sosa that Fernandez used multiple devices to manufacture counterfeit currency.

20. In my training and experience I have come to know that individuals engaged in the sale or transfer of counterfeit US currency often use cellular or mobile telephones to facilitate the crime and such devices often contain evidence of the offense. In this case, there is probable cause to believe that mobile telephone devices used by Fernandez will contain evidence of the offense

and were used to facilitate the transfer of counterfeit currency based on his electronic communications with CI20-02282 using a cellular telephone.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my training and experience, in conjunction with talking with other law enforcement agents, conducting a search of a computer system, documenting the search, and making evidentiary copies of data storage devices is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search. In some cases, it is impossible to even conduct the search without expert technical assistance. Since computer evidence is extremely vulnerable to tampering or destruction through error, electrical outages, and other causes, removal of the system from the PREMISES will assist in retrieving the records authorized, while avoiding accidental destruction of the records. It would be extremely difficult to secure the system on the PREMISES during the entire period of the search. Furthermore, without actually accessing and viewing all computer disks and hard drives, upon which data can be stored, it is impossible to determine what is on such disks and hard drives. Furthermore, when records are stored on floppy disks or on hard drives, even when they have purportedly been erased or deleted, they may still be retrievable through the use of commercially available utility programs or with the aid of expert technical assistance.

22. Accordingly, the removal of the computers and software from the target PREMISES into law enforcement custody to allow a complete analysis of the data in the computer and on its storage media is justified. In order to fully retrieve data from a computer system, the analyst also needs to search all magnetic storage devices as well as the central processing unit. Further, the analyst needs to search all the system software and any applications software, which may have

been used to create the data (whether stored on hard drives or on external disks) for proper data retrieval.

BIOMETRIC AUTHENTICATION ON DIGITAL DEVICES

23. Based on the facts set forth in this affidavit, I believe that the PREMISES to be searched will contain mobile electronic devices such as laptop computers, smartphones, and tablets, which will contain evidence subject to search and seizure under this warrant. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

24. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

25. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on

certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

26. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello. Samsung cellular telephones also have a similar iris-recognition feature.

27. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

28. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, including laptop and cellular devices, will be found during the search. The

passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

29. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period, for example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time

30. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned persons the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices, including to (l) press or swipe the fingers (including thumbs) of the aforementioned persons to the fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in

front of the face of the aforementioned persons to activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of the aforementioned persons to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

31. The passcode or password that may be needed to unlock the digital device(s) found during the search of the PREMISES is not known to law enforcement. Thus, it will likely be necessary to use the fingerprints or thumbprints of the user(s) of any fingerprint sensor-enabled device(s) found during the search, or to place the device(s) in front of an owner's face, in order to unlock the device(s) for the purpose of searching for the evidence subject to seizure under this warrant.

32. Therefore, I request the authority to compel the use of the fingerprint(s) or thumbprint(s) of any person, or to place a device in the face of any person, who is located at the PREMISES during the execution of the search and is reasonably believed by law enforcement to be the user of a fingerprint sensor or facial/retina authentication enabled device located at this residence. The requested authorization is necessary because the government may not otherwise be able to access the data contained on these devices for the purpose of searching for the evidence subject to seizure under this warrant.

CONCLUSION

33. Based upon the foregoing facts, I believe that probable cause exists that **OCTAVIO FERNANDEZ Jr.** did, with the intent to defraud, falsely make counterfeit currency of the United States, and transferred the same with the intent that it be passed, published, and used as true and genuine in violation of Title 18, United States Code, Sections 471 and 473, and that evidence of the commission of these criminal offenses, contraband, the fruits of crime, and

property designed or intended for use which is and has been used as the means of committing a criminal offense, as more fully described in Attachment B, will be found at the PREMISES described in Attachment A, including on any computers, computer media, and wireless telephone devices located therein. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of this PREMISES particularly described in Attachment A for the items listed in Attachment B.

Respectfully submitted,

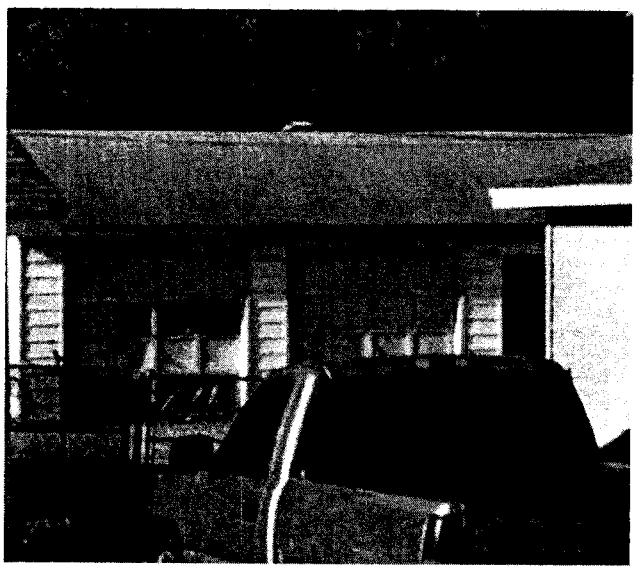
S. Taylor Turnbow
Special Agent
United States Secret Service

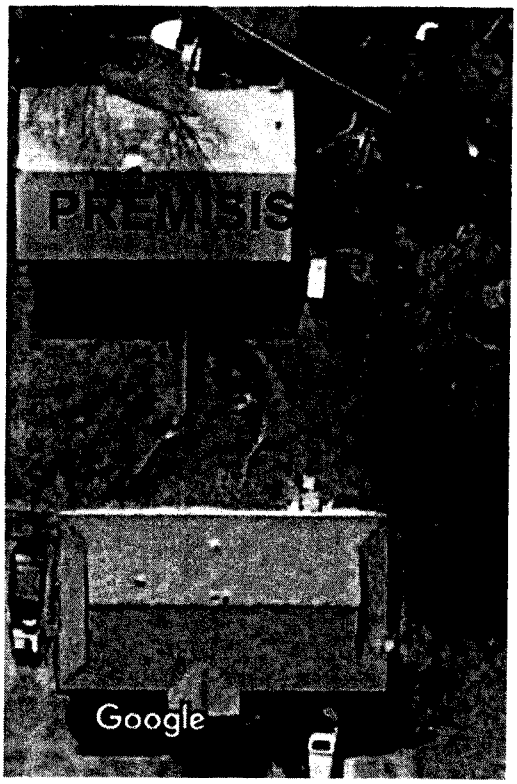
SUBSCRIBED and SWORN to before me this 10th day of October, 2019, at 1:34 am / pm in Fort Worth, Texas

JEFFREY L. CURETON
U.S. MAGISTRATE JUDGE

ATTACHMENT A

Description of the PREMISES to be searched: Detached garage located approximately 50 feet behind the single family residence with the address of 1212 Deridder Street, Fort Worth, Texas, 76106 in Tarrant County. This structure is a single story building with a light colored siding exterior and a grey shingle roof. It has two overhead garage doors and one walk-thru door located on the front of the building and in order to access the premises, entry into the back yard of the main residence must be made through one of two gates, located on either side of the main dwelling as the rear of the property is bound by a fence separating it from a bordering property. The search includes any person(s) located at the premises, and more specifically, the person of **OCTAVIO FERNANDEZ, JR.**, provided that this person is located at subject premises at the time of the search.





ATTACHMENT B

Items believed to be at the PREMISES located at 1212 Deridder Street, Fort Worth, TX 76106, include, but are not limited to the following:

(1) Counterfeit currency, and any evidence of the production thereof.

(2) Pattern note(s) used as template(s) for the production of counterfeit currency.

(3) Property and proceeds from the manufacturing, passing, uttering, and negotiating of counterfeit currency, including cash, money orders, gift cards, and receipts for same.

(4) Records and ledgers, storage facility documents, account books, notes, names and/or code names or nicknames, and/or identifying information reflecting customers, amounts of counterfeit currency bought, sold or manufactured, amounts of money, paid, owed or collected.

(5) Any and all customer lists, other manufacturer or distributor lists, or any notes containing the individual names of such persons, telephone numbers and/or addresses of these customers, manufacturers, or distributors, and any corresponding records of accounts receivable, money paid or received, counterfeit currency supplied or received, cash received to be paid or intend to be paid for counterfeit currency.

(6) Any and all items pertaining to the manufacture, distribution, and possession of counterfeit currency, including: photographs and photography equipment; negatives, motion pictures, videos, and audio tapes related to the production, manufacture, and/or negotiation of counterfeit currency.

(7) Computers and computer equipment, such as hard-drives, floppy disks, external computer drives, computer peripherals, other electronic storage media, printers, and computer scanning equipment; software, copiers; ink and ink cartridges; and receipts for the purchase and/or repair of all these items.

(8) Wireless telephones (or mobile telephone, or cellular telephone or iPhone) capable of transmitting voice communications and a broad range of other capabilities including but not limited to storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.